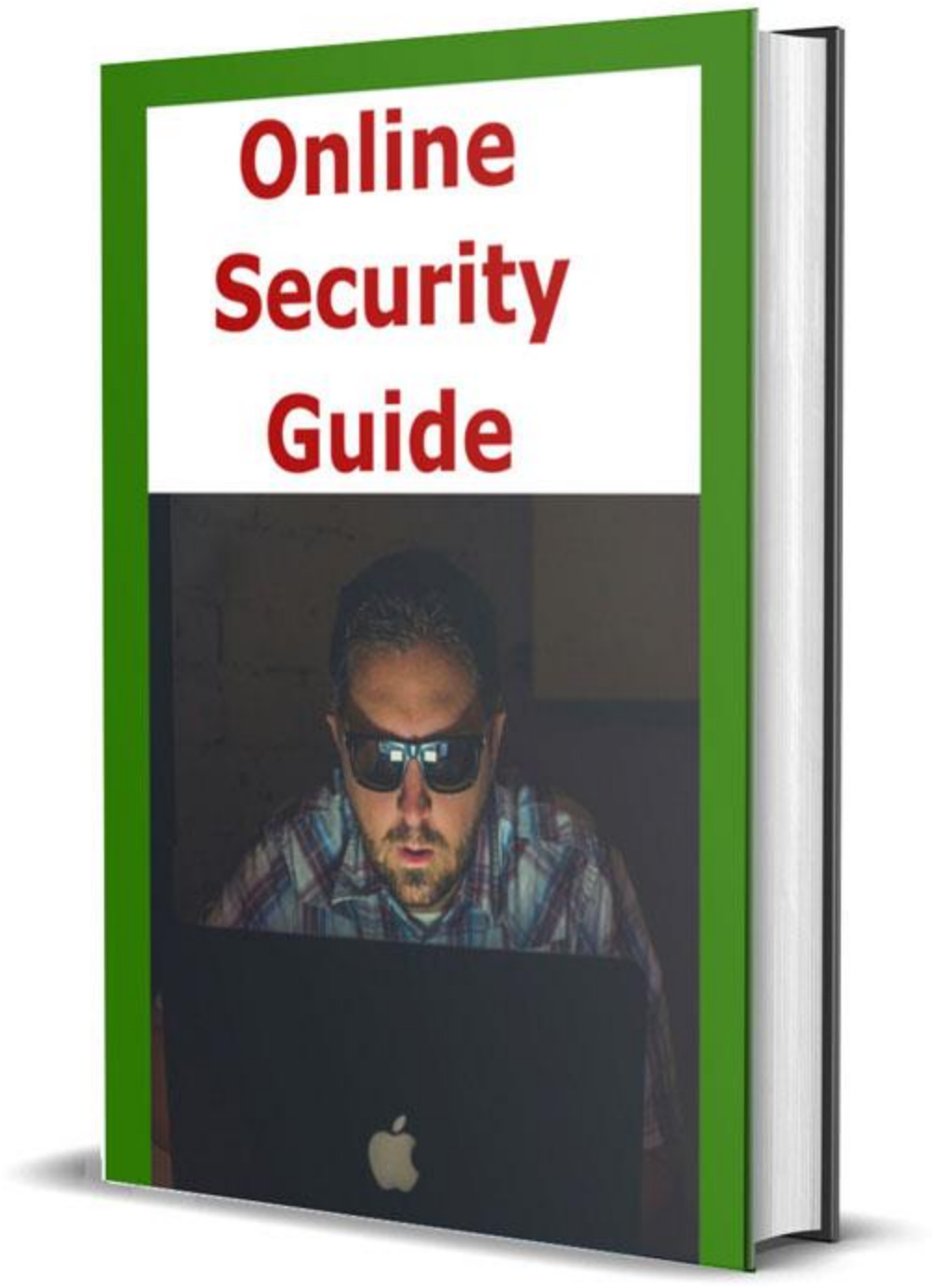
Online
Security
Guide

In today's digital age where hackers and spammers steal personal and financial data from online users, it is crucial to take multiple steps to prevent falling victim and safeguard your online security.

Here’s a comprehensive security guide to help you protect yourself from various online threats.

1. Use Strong Password

Create unique and strong passwords for each of your accounts.

- **Length and Complexity:** Your password should be at least 12 characters long with a good mixture of upper case and lower case letters, numbers, and special symbols.

You can use the password generator to generate a strong password each time you need to create a password.

- **Avoid Common Passwords:** Never use easy passwords like "12345", "letmein", "abcdefg". A

computer can crack these passwords in under a second.

Use the password strength checker to test how secure your password is.

2. Use a Password Manager

- **Store Passwords:** Strong passwords require a password to be long and complex, hence they are hard to remember.
- The average person has about 15 passwords for different accounts, it is almost impossible to remember the passwords.
- It is also a hassle and unsecured to write down the passwords on paper and carry them around.

- **Password Managers:** A password manager like 1Password comes in handy.

- It allows you to securely store all your passwords in one place, and you have only one master password to remember to access the password generator.

Here's a list of recommended password managers that you may consider.

3. Enable Two-Factor Authentication (2FA)

Two-factor authentications involve verifications from a user's email and phone during login that adds an extra layer of security to your accounts.

Most banks, email providers, and online retailers offer two-factor authentication when logging into their systems.

Always enable two-factor authentication so that you keep your account safe.

4. Keep Software Up-to-Date

Keep your operating system, web browsers, and software up to date.

Companies often release updates that fix known bugs and security flaws from their systems.

These flaws might allow hackers to steal data from the user.

You should always install the latest updates on your phone or computer.

Enable automatic updates so you don't have to check for updates manually.

5. Use Antivirus Software

Antivirus software protects you from malware, ransomware, and other virus from your computer.

Your computer may be affected upon visiting a malicious website, installing software, or clicking a link from a spam email.

Scan your computer regularly with reputable antivirus software like Norton, Bitdefender, or Avast.

6. Use a VPN

- **Avoid Public WiFi:** If you ever use public Wifi at a fast food restaurant, coffee shop, or library, you are at risk of losing sensitive information.
-
- Public Wi-Fi networks are often insecure and can be hacked by attackers to steal your data.

- **Use Mobile Data:** Your mobile data is secured, use your mobile data instead of public Wifi for online transactions or online banking.
-

Never use public Wifi to enter your credit card information or access your bank information.

- **Use VPN:** A virtual private network or VPN encrypts your internet traffic and hides your real IP address, encrypting personal data, and making it harder or impossible for hackers to steal your data.
-

Choose a reputable VPN provider like ExpressVPN or NordVPN.

7. Emails & Links

- **Check emails carefully** - Be aware of phishing and spam emails.
-
- Email providers these days do a good job filtering spam mail, but from time to time, phishing emails still land in your inbox.
- Some of these emails may mimic reputable organizations but are actually from spammers.

-
- As soon as you click on the links from these emails, your personal and financial information may be compromised.

- **Check links carefully:** Before clicking on any link on a browser or an email, check the URL and make sure it is indeed the website you want to visit.